УДК 621.391

МАЗУРКОВ М.И.

КОМПОЗИЦИОННЫЙ МАТРИЧНЫЙ ШИФР НА БАЗЕ СОВЕРШЕННЫХ ДВОИЧНЫХ РЕШЕТОК

Одесский национальный политехнический университет,
Украина, Одесса, 65044, пр. Шевченко 1

Аннотация. Предложен композиционный матричный шифр на базе совершенных двоичных решеток, который состоит из четырех парциальных шифров, обладает легко контролируемым уровнем защиты информации от несанкционированного доступа и другими практически приемлемыми вычислительными свойствами

Ключевые слова: криптография, шифр, алгоритм, перестановка, подстановка, совершенная двоичная решетка, уровень защиты информации

Вопросы синтеза и приложения совершенных двоичных решеток (СДР) или perfect binary arrays (PBA) рассматривались в многочисленной литературе, например [1–13] применительно к различным радиотехническим задачам: для синтеза апертуры антенны; построения совершенных частотно-временных кодов; построения новых классов блоковых корректирующих кодов; построения новых классов ортогональных, биортогональных и минимаксных сигналов со свойством многопетлевого циклического сдвига; построения классов минимаксных корректирующих кодов с мажоритарным декодированием, и др.

Целью данной статьи является разработка однораундового и многораундового композиционных матричных шифров на базе полных классов и эквивалентных классов совершенных двоичных решеток.

Совершенной двоичной решеткой называют двумерную последовательность-матрицу

$$H(N)=||h_{i,j}||,\ i,j=\overline{0,N-1},\ h_{i,j}\in\{-1,1\}, \quad (1)$$

имеющую идеальную двумерную периодическую автокорреляционную функцию (ДПАКФ), элементы которой

$$R(\tau_1,\tau_2)=\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}h_{i,j}h_{i+\tau_1,j+\tau_2}=$$

$$=\begin{cases}N^2, & \tau_1=\tau_2=0,\\ 0, & \text{при других } \tau_1 \text{ и } \tau_2,\end{cases} \quad (2)$$

где $\tau_1,\tau_2=\overline{0,N-1}$, $N=2^s$, или $N=3\times 2^s$, s — произвольное натуральное число. Вопросы синтеза различных классов СДР рассмотрены во многих источниках [1–11], из содержания этих работ следует:

Утверждение.

Существует алгоритм [14], который по номеру решетки из полного $U(N)$-класса СДР [1] позволяет восстановить (синтезировать) саму решетку; а также существует алгоритм, который по номеру перестановки из числа $N!$ перестановок позволяет восстановить саму перестановку.